REMARKS

The Examiner is thanked for the performance of a thorough search.

SPECIFICATION

In the specification, the title on page 1 has been amended as follows:

ESTABLISHING A NEW SHARED SECRET KEY OVER A BROADCAST CHANNEL FOR A MULTICAST GROUP BASED ON AN OLD SHARED SECRET KEY

On page 1, a new section titled RELATED APPLICATIONS has been added at the tope of the page and immediately following the title, which includes one new paragraph that cross-references two related co-pending non-provisional applications.

The following paragraphs have been amended to correct typographical errors: page 14, lines 1-5; page 14, lines 15-21; and page 16, lines 3-7. No new matter is introduced.

DRAWINGS

Figure 1 has been amended to include three inadvertently omitted left parentheses in the first three formulas shown in block 116. No new matter is introduced.

STATUS OF CLAIMS

Claims 5, 9, 14, 18, 23, and 27 have been amended.

Claims 34-53 have been added.

No claims have been cancelled or withdrawn.

Claims 1-53 are currently pending in the application.

SUMMARY OF THE REJECTIONS/OBJECTIONS

The title has been objected to as allegedly not descriptive. Claims 8, 17, and 26 have been objected to as being separated by a claim that does not depend from the same dependent claim. Claims 9, 18, and 27 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite. Claims 1, 10, 19, and 28 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent Number 4,531,020 issued to Wechselberger et al. (" *Wechselberger* "). Claims 1, 10, 19, and 28 have been rejected under 35 U.S.C. § 102(e) as

allegedly anticipated by U.S. Patent Number 6,584,566 B1 issued to Hardjono (" *Hardjono* "). Claims 7, 16, and 25 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono*. Claims 6, 15, and 24 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of U.S. Patent Number 6,330,671 B1 issued to Aziz (" *Aziz* "). Claims 2-5, 11-14, 20-23, and 29-31 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of non-patent document entitled "A Course in Number Theory and Cryptography," by Neal Koblitz (" *Koblitz* "). Claim 32 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of Aziz and in further view of *Koblitz*. Claims 9, 18, and 27 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of U.S. Patent Number 6,684,433 B1 issued to Srivastava (" *Srivastava* "). Claims 8, 17, 26, and 33 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of *Koblitz* and in further view of *Srivastava*. The rejections are respectfully traversed.

RESPONSE TO REJECTIONS NOT BASED ON THE PRIOR ART

A. APPLICATION TITLE

The title has been objected to as allegedly not being sufficiently descriptive. In the specification amendment above, the title has been amended to specifically describe establishing a new shared secret key over a broadcast channel for a multicast group based on an old shared secret key. The Applicant respectfully submits that the new title addresses the Office Action's objection.

B. ORDERING OF DEPENDENT CLAIMS

Claims 8, 17, and 26 have been objected to as being dependent claims that depend from a dependent claim and that are separated by claims that do not also depend on the same dependent claim. For example, Claim 8 depends on Claim 2, but Claims 6 and 7 depend on Claim 1. The Applicant apologizes for any confusion created by the ordering of Claims 8, 17, and 26.

However, the Applicant respectfully notes that MPEP §608.01(n)(IV) cited in the Office Action is phrased in terms of "should", not "must." This observation, when taken with

the guidance in both the MPEP and the Office Action that the "applicant's sequence [of claims] will not be changed," does not require that the Applicant reorder the claims via unnecessary amendments that are burdensome under the current amendment practice for both the Applicant to prepare and the Office to enter.

Furthermore, the Applicant notes that MPEP §608.01(n)(IV) recognizes that "the order of claims may change and be in conflict with" the desired order during prosecution, and therefore MPEP §608.01(n)(IV) states that "the numbering of dependent claims and the numbers of preceding claims referred to in dependent claims should be carefully checked when claims are renumbered upon allowance."

Given the additional claims added in the amendment above, many of which are also out of the desired order since similar dependent claims have been added that depend on independent Claims 1, 10, and 19, the renumbering of the claims upon allowance will effectively render this objection moot, and thus the Applicant has not changed the ordering of Claims 8, 17, and 26.

C. 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 9, 18, and 27 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action states that the variable "N" is not defined. Claims 9, 18, and 27 have been amended to include the definition of the variable "N" from page 24 of the Application. The Applicant respectfully submits that the amendments to Claims 9, 18, and 27 traverse the indefiniteness rejection.

In addition, similar amendments to Claims 5, 14, and 23 have been made to explicitly recite within those claims the definitions of variables "y" and "K'" that were included in other claims, but not expressly in Claims 5, 14, and 23 or in Claims 1, 10, and 19 from which Claims 5, 14, and 23 depend.

RESPONSE TO REJECTIONS BASED ON THE PRIOR ART

Claims 1, 10, 19, and 28 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by *Wechselberger*. Claims 1, 10, 19, and 28 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by *Hardjono*. Claims 7, 16, and 25 have been

rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono*. Claims 6, 15, and 24 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of *Aziz*. Claims 2-5, 11-14, 20-23, and 29-31 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view *Koblitz*. Claim 32 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of Aziz and in further view of *Koblitz*. Claims 9, 18, and 27 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of *Srivastava*. Claims 8, 17, 26, and 33 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Hardjono* in view of *Koblitz* and in further view of *Srivastava*. The rejections are respectfully traversed.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

"A method for providing shared secret keys for communicating through a secure channel between members of a dynamically changing multicast group connected over an insecure network, the method comprising the computer-implemented steps of:

computing a first shared secret key for establishing a first multicast group that includes a set of one or more first members;

generating a first multicast group exchange key based on the first shared secret key;

receiving a first user exchange key from a first user requesting entry into the first multicast group;

computing a second secret key *based on* the first user exchange key and the first shared secret key;

sending the first multicast group exchange key to the first user, wherein the first multicast group exchange key allows the first user to generate the second shared secret key; and

establishing a second multicast group whose members include the first user and the set of one or more first members of the first multicast group, wherein the second shared secret key provides a first secure channel for communicating between members of the second multicast group over the insecure network." (Emphasis added.)

Thus, Claim 1 features "**computing a second secret key *based on* the first user exchange key and the first shared secret key**..." In other words, the computing of the second secret key depends upon the first shared secret key. For example, in the embodiment illustrated in FIG. 4, in block 410 the multicast group computes a new shared secret key (e.g., the second secret key of Claim 1) based on the admitted user's exchange key (e.g., the first user exchange key) and the current shared secret key (e.g., the first shared secret key).

As a more specific example, in the embodiment illustrated with respect to FIG. 3B and described in the application on page 14, when Bob 306 wishes to join the multicast that already includes Alice 302, the new shared secret key "k1" (e.g., second shared secret key of Claim 1) is calculated by the current membership of the multicast (e.g., Alice 302) according to the expression $k1 = Y'^{k} \bmod n$, where "Y'" is the exchange key (e.g., first user exchange key) that is supplied by Bob 306, "k" is the initial shared secret key (e.g., the first shared secret key), and "n" is a prime number selected by the members of the multicast and used to previously generate the initial shared secret key, "k." Similarly, as described in the application on pages 15-17 with reference to FIG. 3C and FIG. 3D, when additional members are added (e.g., Carol 314 and Dave 322), new share secret keys are generated based on the previous shared secret key and the exchange key supplied by the member to be admitted to the multicast.

In the approach of Claim 1, with the exception of the initial shared secret key (e.g., the first shared secret key of Claim 1), a subsequent shared secret key is based upon the previous shared secret key. In an embodiment that employs the Diffie-Hellman algorithm (which is described in the Application on page 4), the old shared secret key and the first user exchange key are used by the members of the multicast group when generating a new shared secret key. Thus, the approach of Claim 1 is fundamentally different than the prior approach described in the Application on pages 4-5 for using Diffie-Hellman for a multicast in which each member

of the multicast group selects a secret random large number (e.g., "a", "b", and "c"). The multicast members then use that secret random large number to generate public keys that are shared and ultimately used to determine a new secret key, "k," and therefore the new secret key is not based on the old secret key in the prior approach.

(2) DISCUSSION OF *WECHSELBERGER*

In contrast to Claim 1, *Wechselberger* generally discloses a "multi-layer encryption system for the broadcast of encrypted information." (Title.) More specifically, *Wechselberger* discloses "a system for enciphering and deciphering digital information signals...in the field of broadcast television," (Col. 1, lines 7-9) and a "method of controlling the simultaneous broadcast of enciphered digital information signals, for example in a radio or television broadcast environment, to a plurality of subscribers" using "several levels of enciphering keys." (Abstract.)

In *Wechselberger*, the digital information signals are enciphered using a "service key" that is used for a specific program or a specific channel and that is changed on a periodic basis. (Col. 2, lines 10-20.) The broadcaster communicates with all the subscribers in a group using a "group key" and thereby can change the service key used by the subscribers or a program or channel. (Col. 2, lines 20-31.) Alternatively, the decoder at each subscriber can store a large number of service keys with the broadcaster communicating using the group key to tell subscribes which service key to use. (Col. 2, lines 31-35.) The group key also is used to reform groups, add or delete subscribers, or to change the group key. (Col. 2, lines 36-44.) Finally, each subscriber has a hard wired "box key" that is peculiar to a specific describer that allows the broadcaster to privately communicate with a specific subscriber, such as to change the group key. (Col. 2, line 60 - Col. 3, line 6.)

Thus, there are three layers in the approach of *Wechselberger*, with a key for each layer as follows: a service key used for a specific program or channel sent from the broadcaster to the subscribers; a group key for the broadcaster to communicate with the subscribers in a group; and a box key for the broadcast to communicate with each subscriber individually. As for generation of the different keys, *Wechselberger* merely discloses that key generator 20 provides "a constant supply of enciphering keys," (Col. 3, lines 35-41), without disclosing anything further about how the keys are generated.

(3) THE OFFICE ACTION'S CITATIONS FROM *WECHSELBERGER*

The Office Action states that *Wechselberger* discloses "a step for computing a first shared secret key (abstract), a generating step (abstract), a receiving step (abstract), a step for computing a second secret key (abstract), a sending step (abstract), and an establishing step (abstract)." The hand annotations to the Abstract in the copy of *Wechselberger* supplied with the Office Action indicate that the Office Action rejection is based on equating the following features of Claim 1 to the identified portions of the Abstract of *Wechselberger*: first shared secret key = service key; second shared secret key = change in the service key; first user exchange key = box key; first multicast group exchange key = group enciphering key; and second multicast group exchange key = the group enciphering key may be changed at one or more subscribers.

However, Claim 1 features "computing a second secret key based on the first user exchange key and the first shared secret key." Using the Office Action's analogies based on the Abstract of *Wechselberger*, this would mean that *Wechselberger's* "change in the service key" is computed based on the "box key" and the "service key," which is clearly not the case. There is nothing in *Wechselberger* to indicate that a new service key is based on an old service key, and in fact, there is nothing in *Wechselberger* that indicates how the service keys or any of the other keys are generated. Furthermore, nothing in *Wechselberger* suggests that the new service key is based on the hard wired box key that is unique to each subscriber.

While *Wechselberger* discloses using different layers of keys between a radio or television broadcaster and a group of subscribers, this does not relate to computing a new shared secret key based on a user exchange key and an old share secret key, as featured in the claims of the present application. *Wechselberger* does not disclose, teach, suggest, or in any way render obvious "**computing a second secret key *based on* the first user exchange key and the first shared secret key**..." as featured in Claim 1.

(4) DISCUSSION OF *HARDJONO*

In contrast to Claim 1, *Hardjono* generally discloses "distributed group key management for multicast security." (Title.) More specifically, *Hardjono* discloses an initiator key server that distributes a first key set to a plurality of key servers. (Col. 3, lines 14-15.) The key set includes both an initial common group key and a replacement

common group key. (Col. 3, lines 15-16.) Each key server initially distributes just the initial common group key to the key server's clients that are members of a multicast group, with the initial common group key used for multicast messages. (Col. 3, lines 15-21.) When the need arises to re-key the current common group key for the multicast group, each key server distributes the replacement common group key to the key server's client that are members of the multicast group, with the replacement common group key thereafter used for multicast messages instead of the initial common group key. (Col. 3, lines 21-26.) In addition, the initiator key server shares a private key with each key server (Col. 5, lines 48-55), and each key server shares a domain key with members of the domain (Col. 5, lines 56-63.)

Thus, in the approach of *Hardjono*, two group keys are distributed from a particular key server to a set of additional key servers, which in turn distribute just the first group key to multicast members. When the group key needs to be changed, the additional key servers distribute the replacement group key that was previously distributed by the particular key server. As for the generation of the group keys, *Hardjono* merely discloses that the key server of the initiator of the multicast group (referred to as the Initiator Key Server or IKS) controls the key generation, (Col. 4, lines 30-33), without disclosing anything further about how the keys are generated.

(5) THE OFFICE ACTION'S CITATIONS FROM *HARDJONO*

The Office Action states that *Hardjono* discloses "a step for computing a first shared secret key (abstract; column 3, lines 10-26; and figure 5, element 505), a generating step (abstract; column 3, lines 10-26; and figure 5, element 530), a receiving step (abstract; column 3, lines 10-26; and figure 5, element 530), a step for computing a second secret key (abstract; column 3, lines 10-26; and figure 5, element 505), a sending step (figure 5, element 530), and an establishing step (abstract; column 3, lines 10-26; and figure 5, elements 525 and 530)." The hand annotations to the Abstract and the copy of FIG. 5 on the cover page in the copy of *Hardjono* supplied with the Office Action indicate that the Office Action rejection is based on equating the following features of Claim 1 to the identified portions of the Abstract of *Hardjono*: first shared secret key = initial common group key; second shared secret key = replacement common group key; first user exchange key = member key; and multicast group exchange key = new domain key.

However, Claim 1 features "computing a second secret key based on the first user exchange key and the first shared secret key." Using the Office Action's analogies based on the Abstract and cover page copy of FIG. 5 of *Hardjono*, this would mean that *Hardjono's* "replacement common group key" is computed based on the "member key" and the "initial common group key," which is clearly not the case. There is nothing in *Hardjono* to indicate that the replacement common group key is based on the initial common group key, and in fact, there is nothing in *Hardjono* that indicates how the common group keys or any of the other keys are generated. Furthermore, nothing in *Hardjono* suggest that the replacement common group key is based on the member key that is unique to each subscriber.

While *Hardjono* discloses distribution of initial group keys to clients through key servers with replacement group keys only distributed to clients by the key servers when necessary, this does not relate to computing a new shared secret key based on a user exchange key and an old share secret key, as featured in the claims of the present application. *Hardjono* does not disclose, teach, suggest, or in any way render obvious "**computing a second secret key *based on* the first user exchange key and the first shared secret key**..." as featured in Claim 1.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *WECHSELBERGER AND HARDJONO*

Because *Wechselberger* and *Hardjono*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious "**computing a second secret key *based on* the first user exchange key and the first shared secret key**...", the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 10, 19, 28, AND 29

Claims 10, 19, 28, and 29 contain features that are similar to those described above with respect to Claim 1. In particular both Claim 1 and Claims 10, 19, and 28 feature "**computing a second secret key *based on* the first user exchange key and the first shared secret key**." Similar to Claim 1, Claim 29 features "**the first member to generate a second secret key *based on* the first user exchange key and the first shared secret key**." Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant

respectfully submits that Claims 10, 19, 28, and 29 are allowable over the art of record and are in condition for allowance.

C. CLAIMS 2-9, 11-18, 20-27, AND 30-53

Claims 2-9, 11-18, 20-27, and 30-33 are dependent upon Claims 1, 10, 19, and 29, respectively, and Claims 34-36, 37-39, 40-42, and 43-53 are dependent upon Claims 1, 10, 19, and 28, respectively, and thus include each and every feature of the corresponding independent claims. Each of Claims 2-9, 11-18, 20-27, and 30-53 is therefore allowable for the reasons given above for the Claims 1, 10, 19, 28, and 29. In addition, each of Claims 2-9, 11-18, 20-27, and 30-53 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2-9, 11-18, 20-27, and 30-53 are allowable for the reasons given above with respect to Claims 1, 10, 19, 28, and 29.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Craig G. Holmes
Reg. No. 44,770

Date: April 29, 2004

1600 Willow Street
San Jose, CA 95125
Telephone: (408) 414-1080, ext. 207
Facsimile: (408) 414-1076

Attachments

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on 4-29-04 by